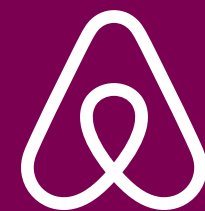
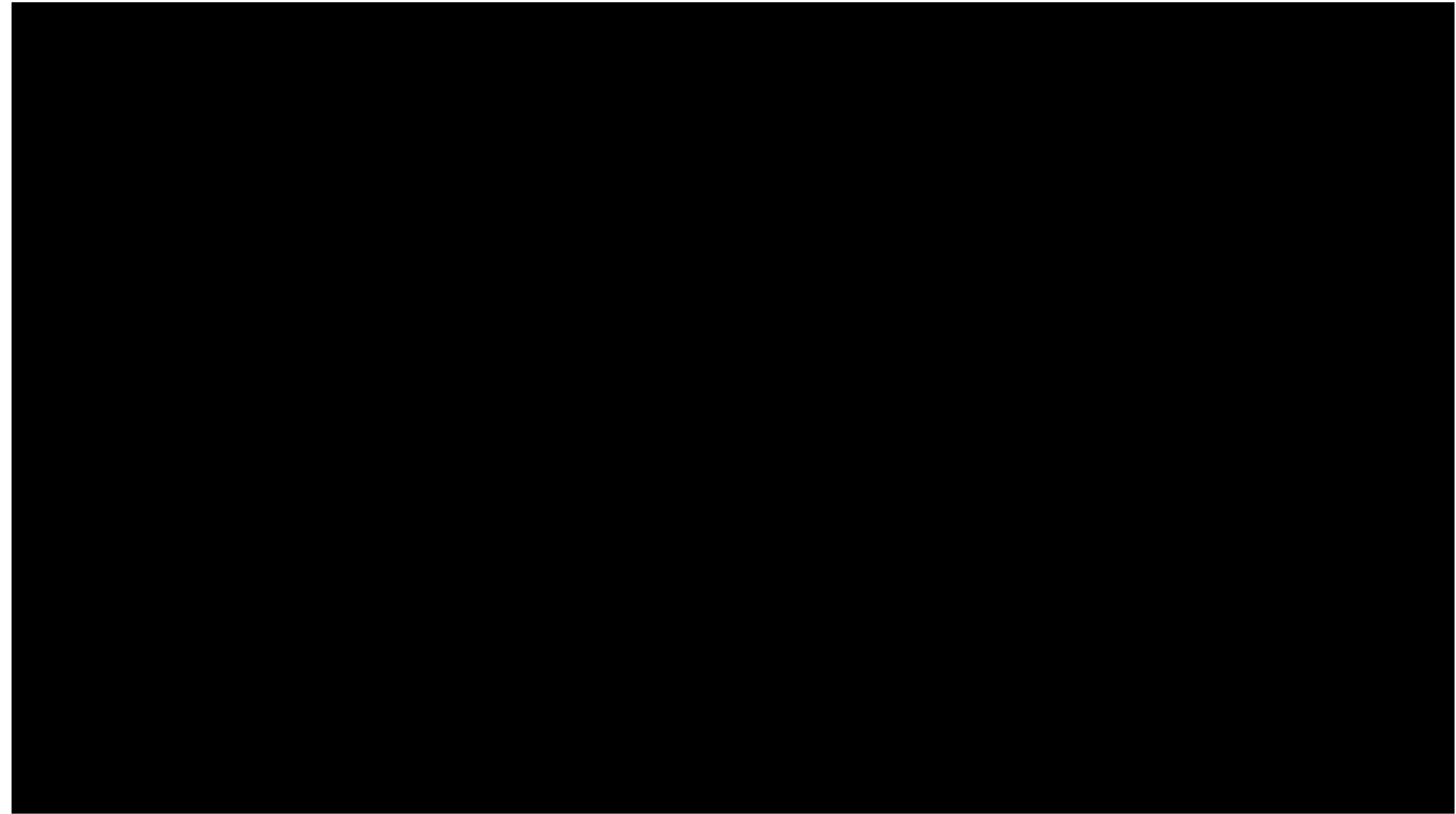


Embracing the adventure with MicroMDM



BRETT DEMETRIS & GRAHAM GILBERT



[GRAHAM.AT/MOVEMBER](https://www.graham.com/movember)

**graham.at/
movember**



DAY 11



MOVEMBER.COM



careers.airbnb.com

The old stack



Configuration Management (Puppet)



Patch Management (Munki)

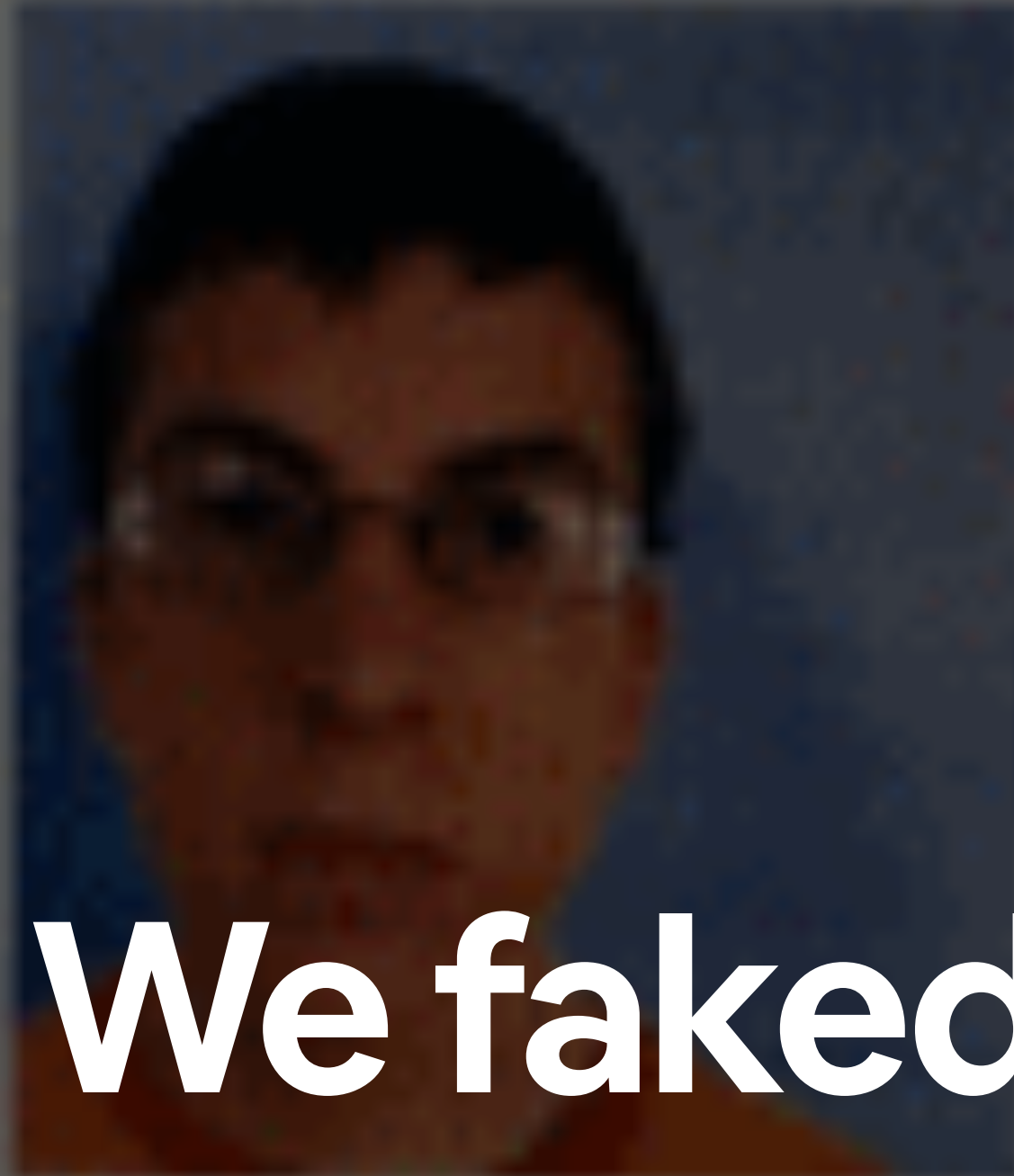


Imaging Solution (Imagr)



Mobile Device Management

What about kernel extensions?



HAWAII

DRIVER
LICENSE

NUMBER 01-47-87441

DOB 06/03/1951 EXP 06/03/2008

SEX HT HAIR EYES SEX CTR

M 5-10 B BRN BRN M 6

We faked it during imaging



McLOVIN
882 MOHONA ST
HONOLULU, HI 96826

McLovin

Then 10.13.2 came along

User Approved MDM

How about MicroMDM?

IT'S FREE RIGHT?



Actually the head of IT Budget and Vendor



Step 1:

Becoming an MDM Vendor



Find the right person on your Enterprise Developer account.



Speak to one or many people at Apple.



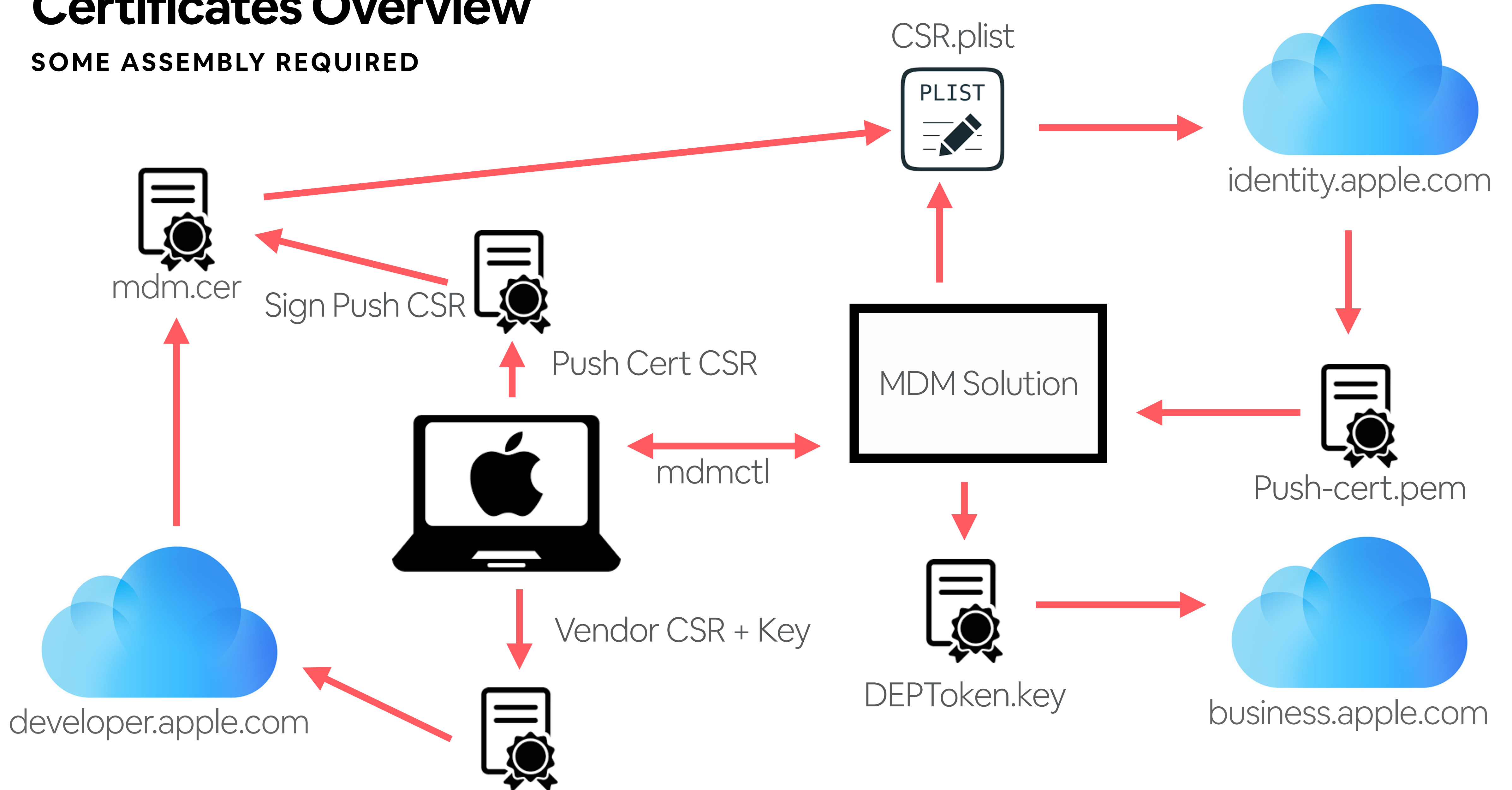
Get your vendor certs.



Bask in glory.

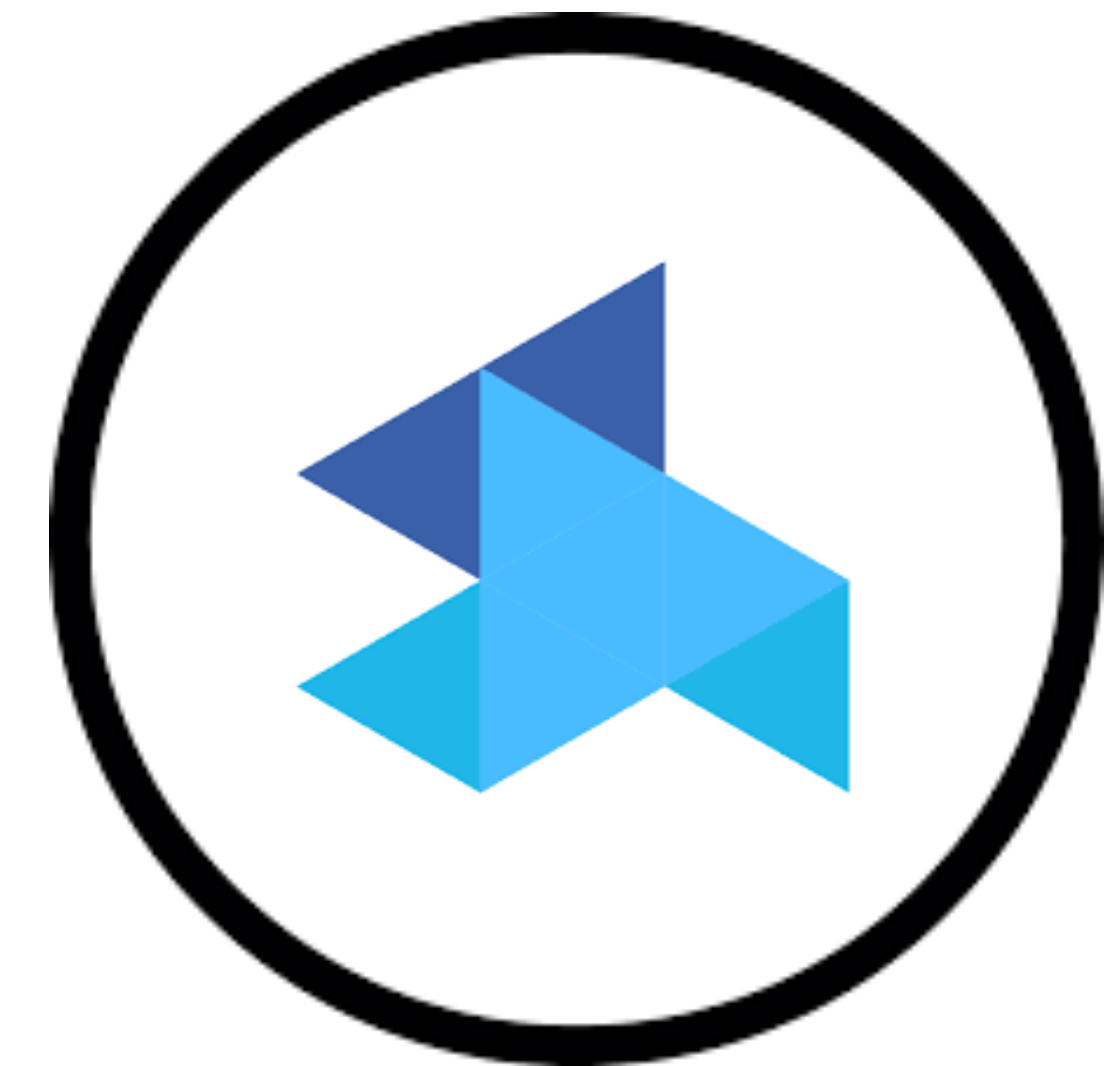
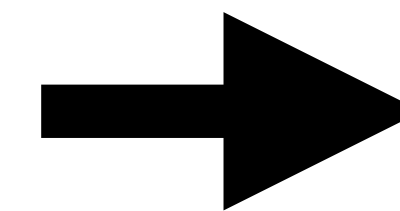
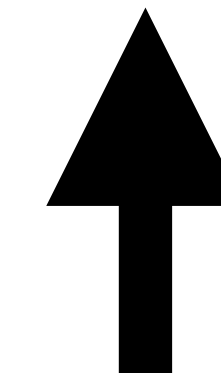
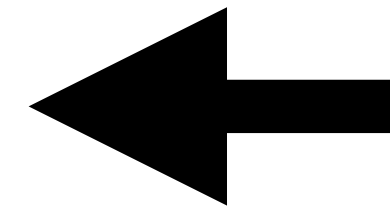
Certificates Overview

SOME ASSEMBLY REQUIRED



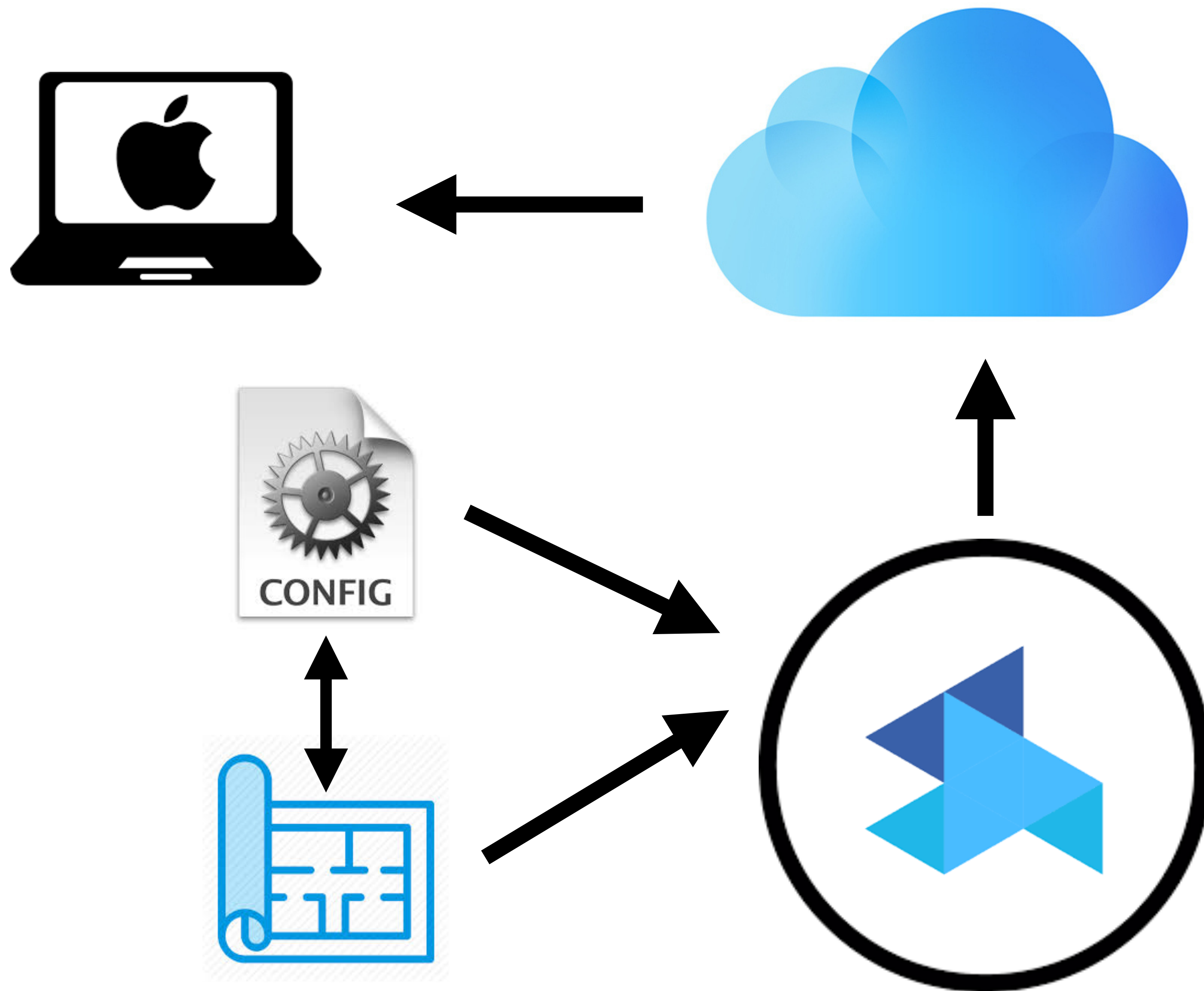
**What does it mean
to become an
MDM vendor?**

FILL IN THE BLANK!



Okay, let's do this

DEP AND CHILL



But What About All The Other Devices?



Script that looped over all the devices and shot out the profile



Repeat previous step a few times



Hope devices come online



Enrollment blueprint deployed profiles ~80% of the time

**Then we needed to
push a password
policy profile**

When all you have is a hammer...

- Sal is our reporting tool
- Sal reports on installed profiles
- Sal can run code in plugins
- I know how to post profiles to MicroMDM with Python
- Sal is in the same VPC as MicroMDM
- Sal is looking like a petty sexy hammer right now...

**What happens if your
MDM doesn't support
something?**

You're doing it yourself.

CLIENT

SAC

[Profiles] machine

Plugin

Have: Serial
Want: UUID
Send: UUID of device profile

MicroMDM
device endpoint
Command endpoint

Do you have the UUID?


NO.


Yes
No


UUID of prof
Base64 enc. profile

2104.0	8577
2105.0	14


Sip


9211



41


0



Gatekeeper

9249


0


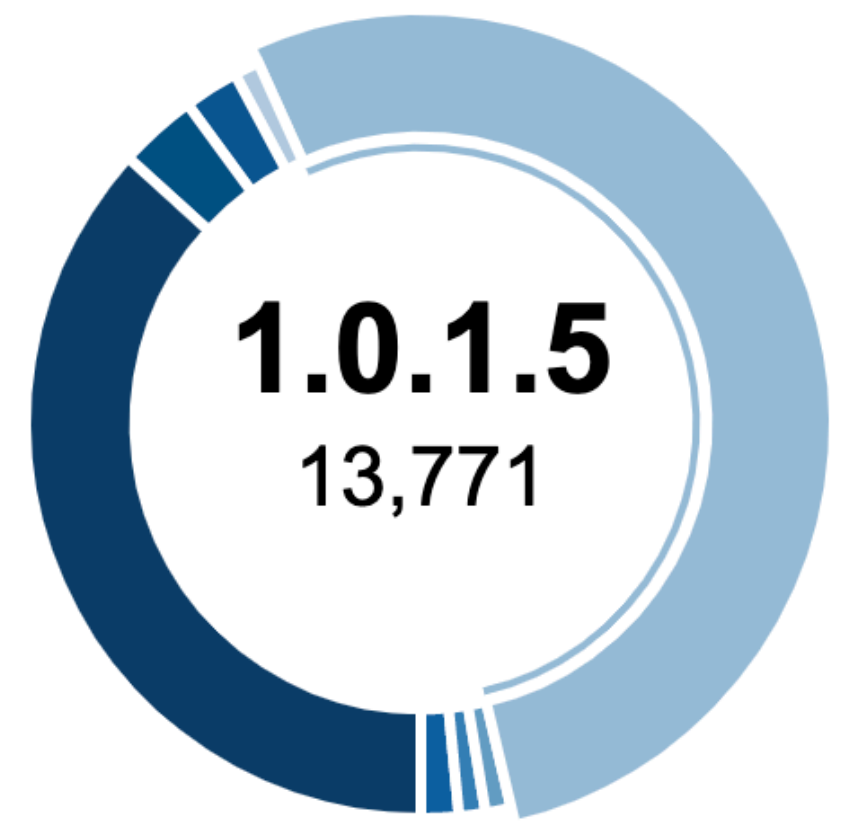
1096


Machine Models




MacBookPro
7,653

Sal Scripts Version



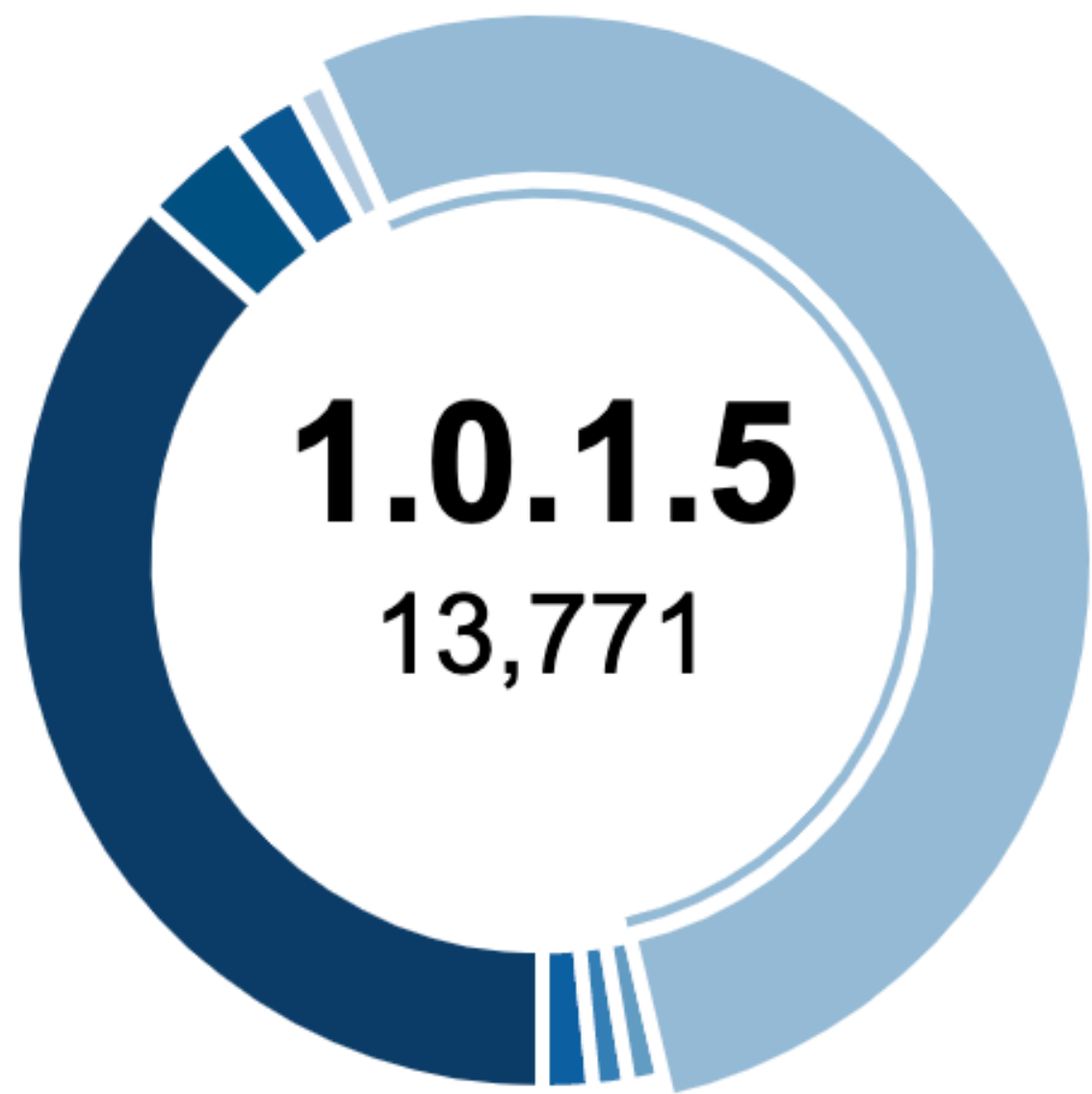
1.0.1.5
13,771

Profile enforcer



MacBookPro
7,653

Sal Scripts Version

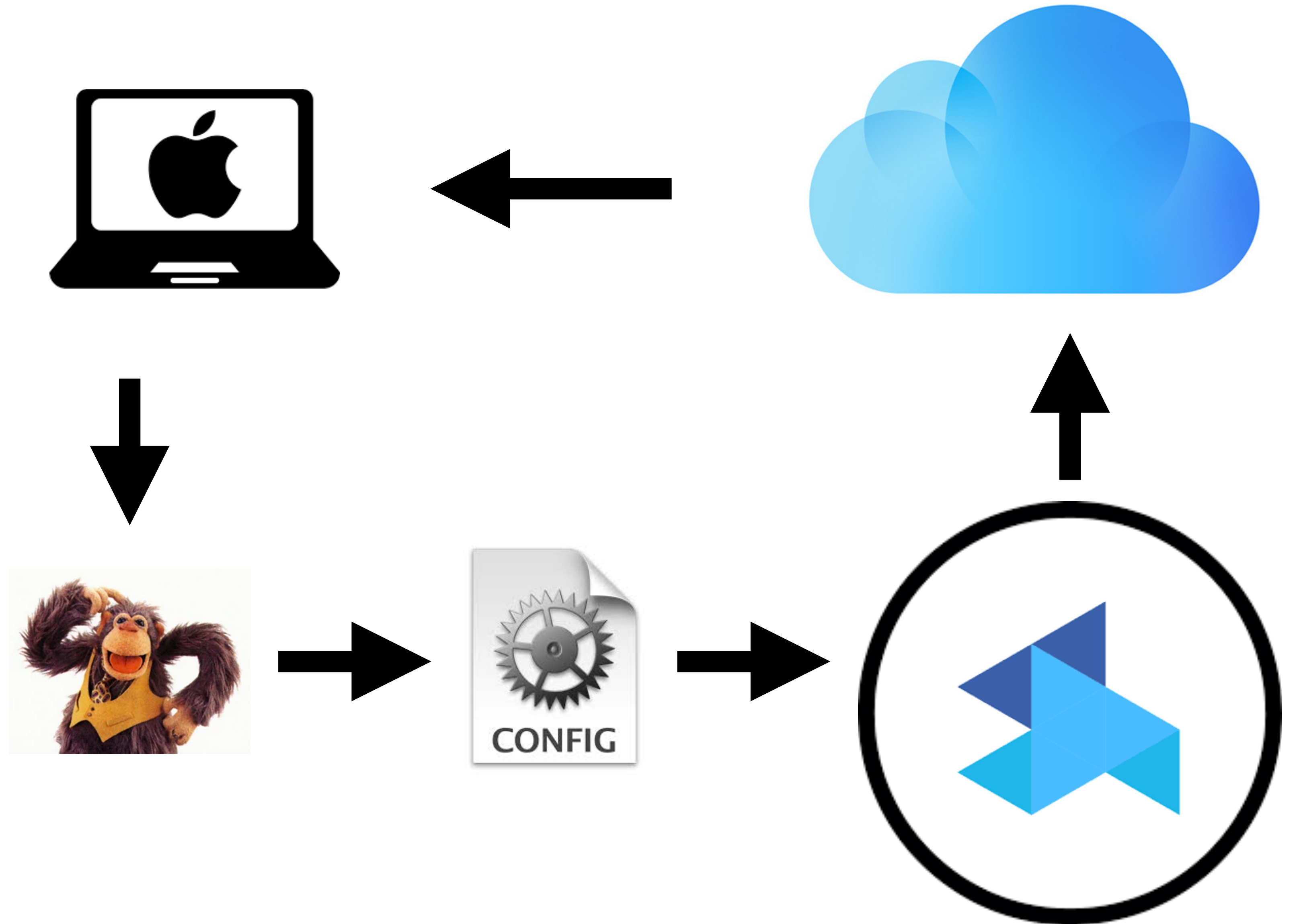


Profile enforcer





Push it, push it real good





A group of men are running down a city street. In the center, a man in a blue suit holds a glowing red orb. To his left, a man in a tan jumpsuit also holds a glowing red orb. Other men in various attire are running alongside them. The background shows city buildings and a street sign.

WHO YOU GONNA CALL?

Nobody

WHO YOU GONNA CALL?



Looking at an MDM Incident

WHAT'S IN PANDORA'S BOX?

MDM Incident

DAY 0

What we Know

- Support has reported that devices are not able to pass Device Enrollment screen
 - New Hire class of ~50 people are starting in 3 business days
- MicroMDM's service is up and logging
 - MicroMDM's database is 22 GB
 - InstallProfile actions are depleted by ~90%
 - SCEP/PKI Operations are taking up to 2min to complete

Action Items

- Read up on BoltDB documentation to understand the database size issue
- Disable Profile Plugin in Sal

MDM Incident

DAY 1

What we Know

- BoltDB is a key value store in written in pure golang
 - There is a compression tool built into the boltldb binary
 - There are several projects for inspecting the database
- Database Compression has no effect
 - The size of the database correctly reflects its contents

Action Items

- Review MDM Specification
- Review MicroMDM code to understand how the command queue works
- Pull a development database, and review MicroMDM's table layout

MDM Incident

DAY 2

What we Know

- BoltDB runs out of memory
 - A database size greater than the server's memory is the main cause of our service interruption
- The MDM Spec lists several status codes in the results payload
 - Acknowledged, Error, CommandFormatError, Idle, NotNow
- MicroMDM's command queue is cumulative based on the MDM response status

Action Items

- Resize AWS instance for MicroMDM to something greater than 22 GB of memory
- Work on reducing the size of MicroMDM Database

MDM Incident

POST MORTEM (BEER TIME)

Action Items

- Write a database tool to clean our the command queue
- Rethink our use of the Sal Plugin

Lessons Learned

- We need a firm understanding of the MicroMDM code base
- We need a complete understanding of the MDM Spec
- We should probably get better at Golang
- Being an MDM Vendor is Hard



MDM is not great

A photograph of a doll lying on its back on a bed of wood chips. The doll is wearing a pink and yellow jacket, black pants, and pink and black striped socks. The text "Not Now" is overlaid in white, bold, sans-serif font across the center of the doll's body. The background is a textured surface of brown wood chips.

Not Now

DEP is never down

**Most of what we need
isn't even possible
with MDM**

Mobile Device Management

Maybe Device Management

Getting Help

The best place to get help with setting up and ongoing maintenance of MicroMDM is the MacAdmins Slack. Join by getting an [invitation here](#).

Once you join Slack, the following channels will be useful.

- `#micromdm` for MicroMDM specific questions.
- `#mdm` and `#dep` for generic questions about MDM and deployment programs.

For defects and feature requests, please [open an issue](#).

Not a product!

MicroMDM is not a full featured device management product. The mission of MicroMDM is to enable a secure and scalable MDM deployment for Apple Devices, and expose the full set of Apple MDM commands and responses through an API. But it is more correct to think of MicroMDM as a lower level dependency for one or more products, not a solution that lives on its own.

For example, MicroMDM has no high level options for configuration profiles. It accepts an already composed `mobileconfig` file and queues it for a single device at a time. Device Management products often have built-in support for signing profiles or pushing them to a chosen device group. MicroMDM expects those features to exist in a higher level companion service.

MicroMDM has no Web UI.

MicroMDM can enable disk encryption and escrow a secret, but it has no option for storing that secret on the server.

Dynamic enrollment / user authentication workflows belong in an external service. MicroMDM serves the exact same enrollment profile at the `/mdm/enroll` server endpoint for every device. It also does not care about how the enrollment is protected from unauthorized devices. The number of possible workflows are infinite, and the recommendation is to point the devices at a separate URL for serving the enrollment profile.

As you see, MicroMDM itself lacks many features that are usually present in device management products. But it also exposes a low level API that would allow an organization to build a product that is highly custom to ones environment. Over time, the community will likely share solutions that depend on MicroMDM and expose higher level workflows.

Before using MicroMDM, consider that there are a number of alternative, commercial products like Airwatch, SimpleMDM and

[invitation here.](#)

Once you join Slack, the following channels will be useful.

- `#micromdm` for MicroMDM specific questions.
- `#mdm` and `#dep` for generic questions about MDM and deployment

For defects and feature requests, please [open an issue](#).

Not a product!

MicroMDM is not a full featured device management product. The mission is to simplify MDM deployment for Apple Devices, and expose the full set of Apple MDM APIs. But it is more correct to think of MicroMDM as a lower level dependency for a product of its own.

For example, MicroMDM has no high level options for configuration profiles, it just pushes a file and queues it for a single device at a time. Device Management products typically push them to a chosen device group. MicroMDM expects those features

~~**We needed it to be a product**~~

We needed a product

Blueprints

- Blueprints specify actions to take when the device enrolls
- Blueprints are a one shot - no ongoing management
- If they work, great
- If not...
- Well, it's mdm

Let's talk about APNS

- Fun fact: devices rarely check in on themselves
- And the schedule they do is completely undocumented
- No way to trigger a checkin from the device
- APNS is the only way we can trigger an MDM checkin
- Good job we control all of the networks our devices are used on...

I heard you like updating profiles

- No versioning built into profiles
- Apple expects us to use the UUID as a version
- Or keep track what profiles have been sent

Profiles: The gift that gives one time

- Profile payloads are evaluated **during install only**
- Too bad if the profile payload isn't supported on the OS you're running
- Even worse if it is supported, but something else changes the setting out from under the profile

We needed it to be a product

MicroMDM Webhooks

Webhooks

macgitecu edited this page 27 days ago · 12 revisions

One of the [design goals](#) of MicroMDM is to provide a way for administrators to subscribe to events generated from the MDM interactions between client & server. The webhook functionality helps to facilitate this process by allowing you to subscribe to the MDM events being sent up to the server. These event notifications provide the flexibility needed to build higher level workflows on top of MicroMDM.

Configuration

In order to enable the webhook callbacks an additional parameter needs to be passed to the `micromdm serve` command.

```
sudo micromdm serve \  
  -server-url=https://my-server-url \  
  -api-key MySecretAPIKey \  
  -filerepo /path/to/pkg/folder \  
  -command-webhook-url https://my-webhook-server-url/webhook
```

The `command-webhook-url` can be either a http or https url. Once configured, MicroMDM will send events to the URL specified.

Example Code

Creating a simple webhook listener is as simple as listening for the POST requests from MicroMDM. Below is an example of a python [Flask](#) server that just prints out all the messages it receives.

► Pa

Home
Troubleshooting
Sign up
Renewal
Forums
Running
Webhooks
Con

Clone

https

AN OPINIONATED MDM ORCHESTRATOR

MDMDirector

What does MDMDirector do?

- Handles initial device enrollment (InstallApplication, InstallProfile, DeviceConfigured)

What does MDMDirector do?

- Handles initial device enrollment (InstallApplication, InstallProfile, DeviceConfigured)
- Profile state management

What does MDMDirector do?

- Handles initial device enrollment (InstallApplication, InstallProfile, DeviceConfigured)
- Profile state management
- Dynamic profile signing

What does MDMDirector do?

- Handles initial device enrollment (InstallApplication, InstallProfile, DeviceConfigured)
- Profile state management
- Dynamic profile signing
- Shared Profiles and Apps

What does MDMDirector do?

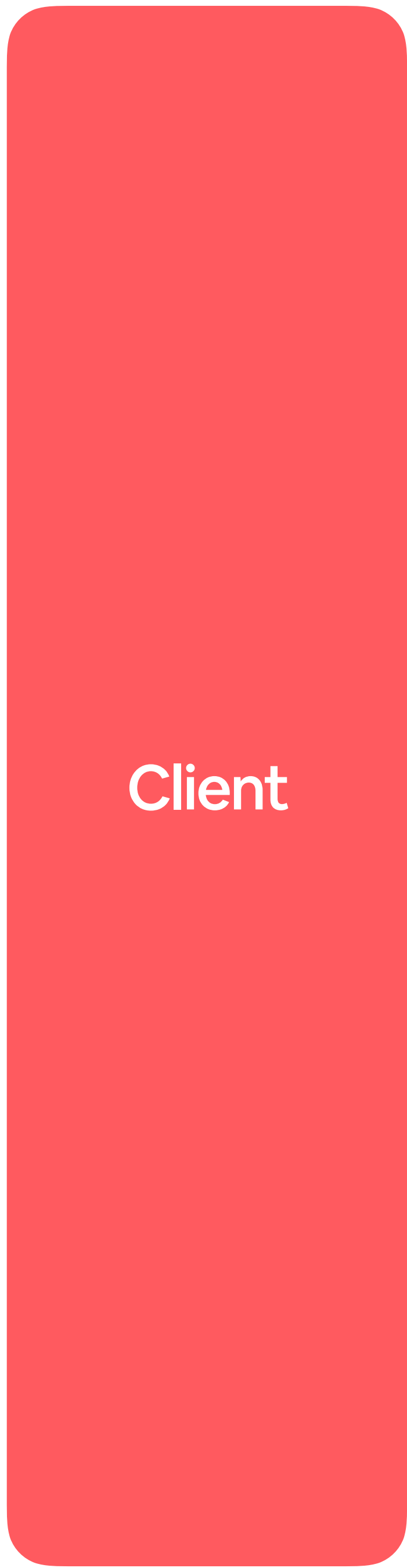
- Handles initial device enrollment (InstallApplication, InstallProfile, DeviceConfigured)
- Profile state management
- Dynamic profile signing
- Shared Profiles and Apps
- Device Profiles and Apps

What does MDMDirector do?

- Handles initial device enrollment (InstallApplication, InstallProfile, DeviceConfigured)
- Profile state management
- Dynamic profile signing
- Shared Profiles and Apps
- Device Profiles and Apps
- RESTful API

What MDMDirector doesn't do

- No GUI
- No groups
- Little flexibility out of the box



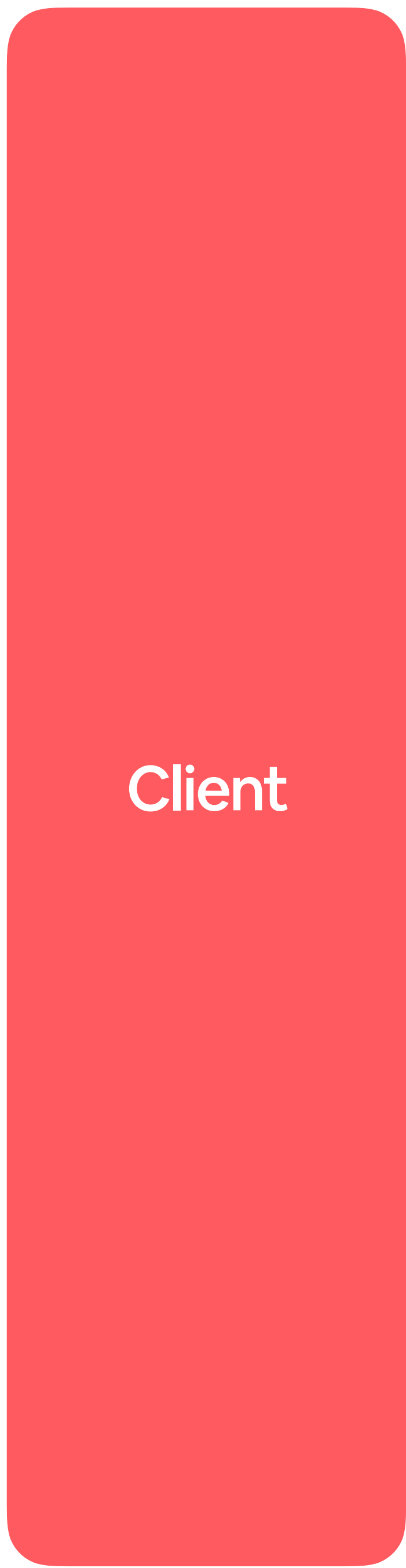
Client

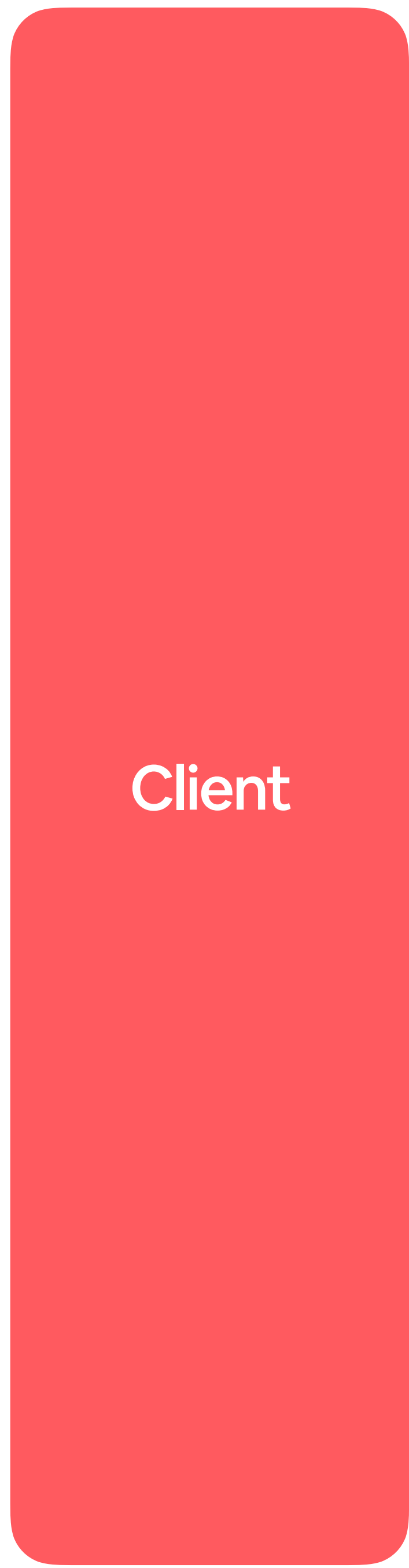


MicroMDM



MDMDirector



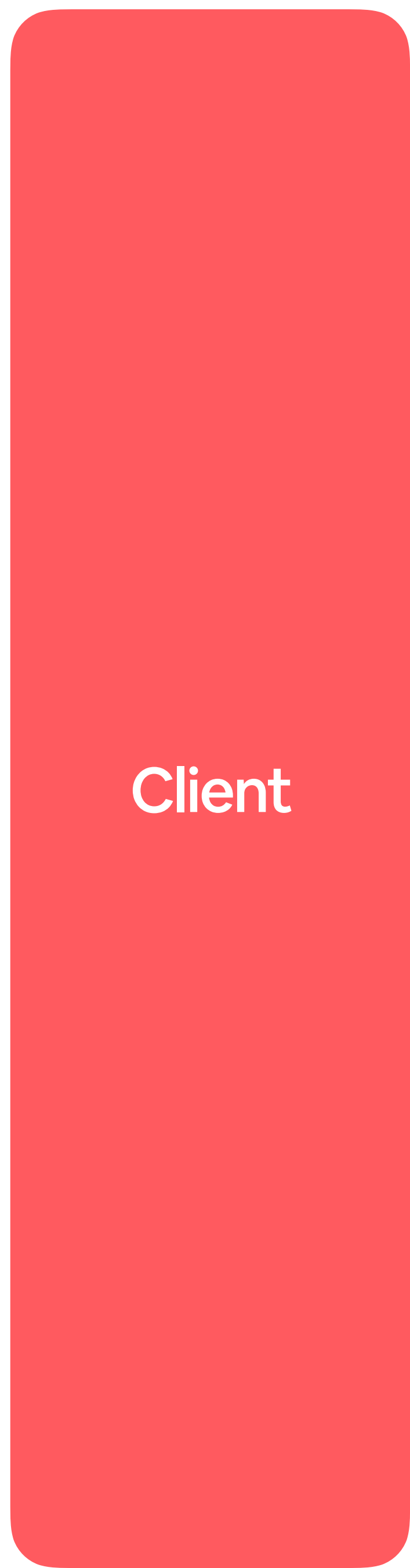


ProfileList



ProfileList





ProfileList



ProfileList

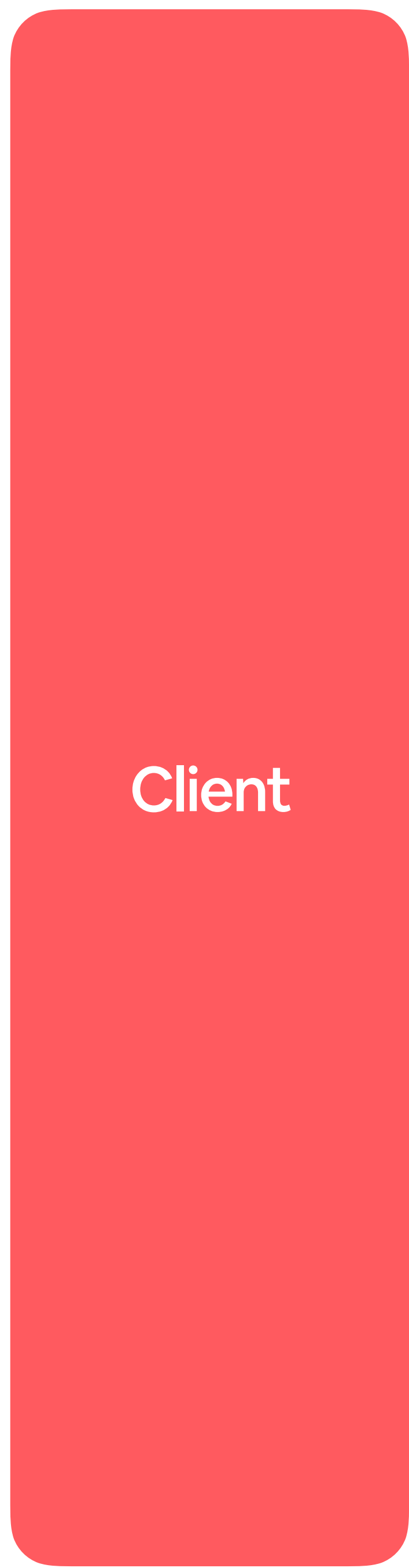


ProfileList



ProfileList





ProfileList



ProfileList

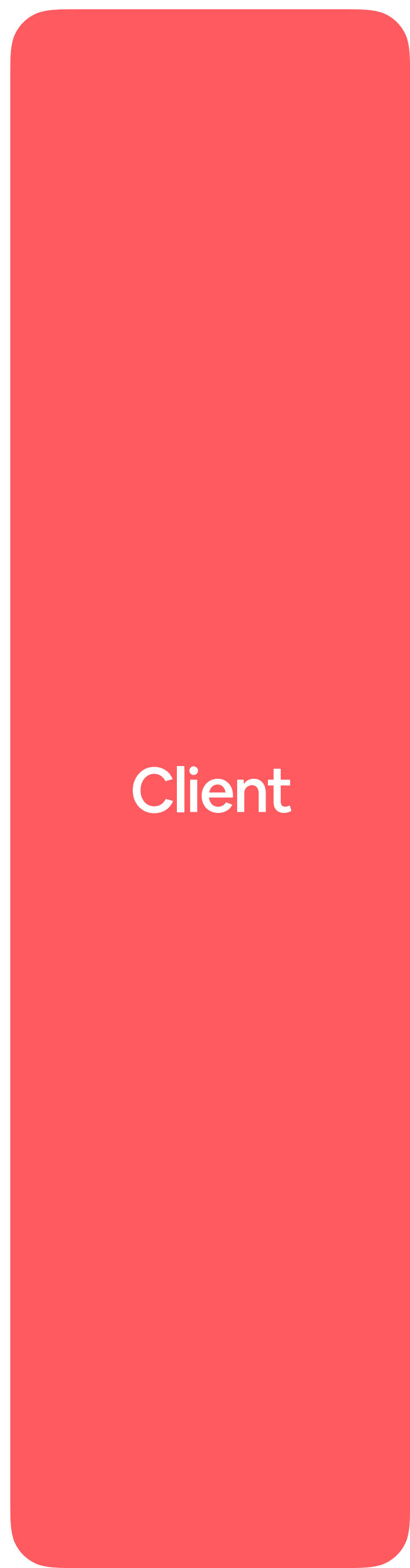


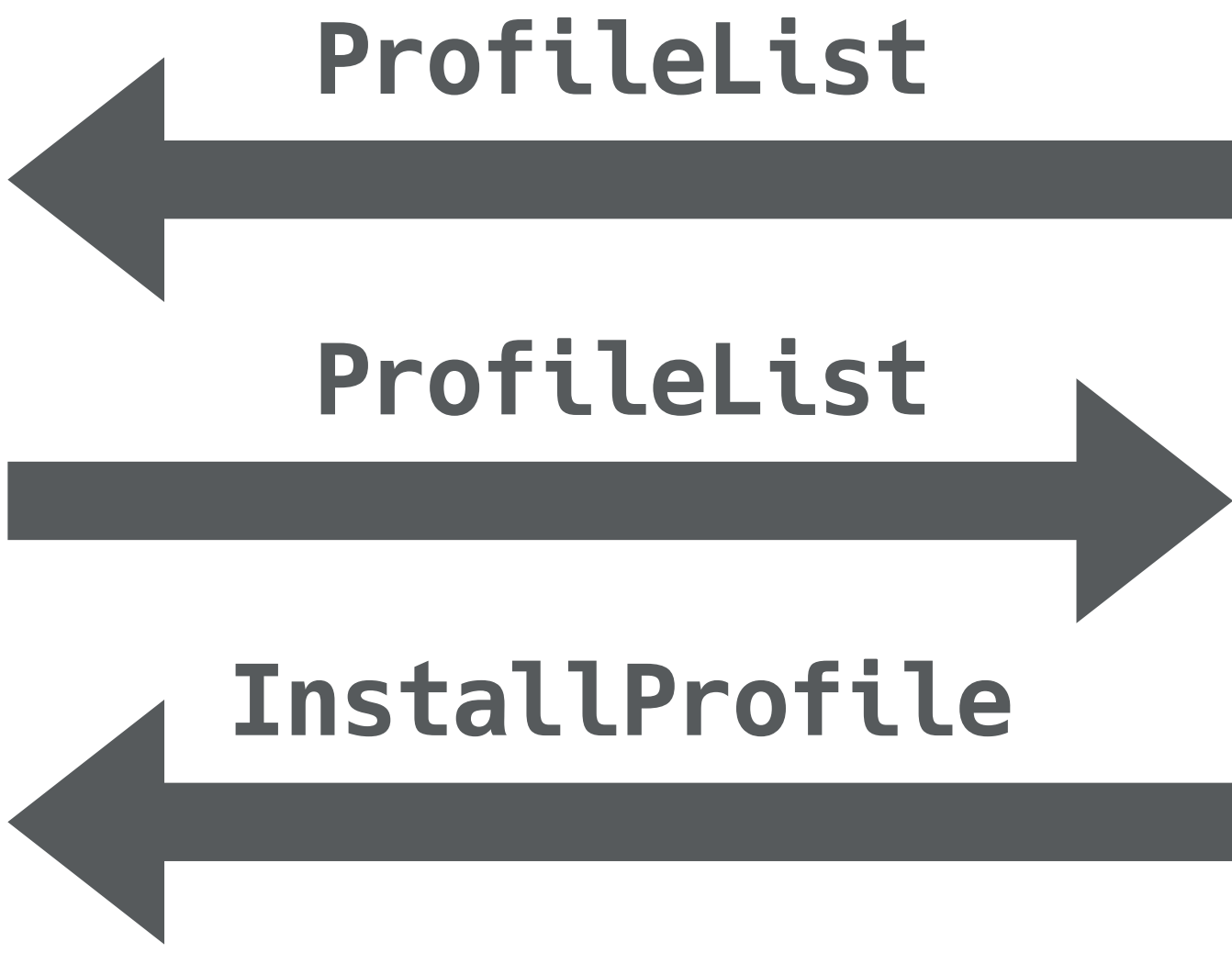
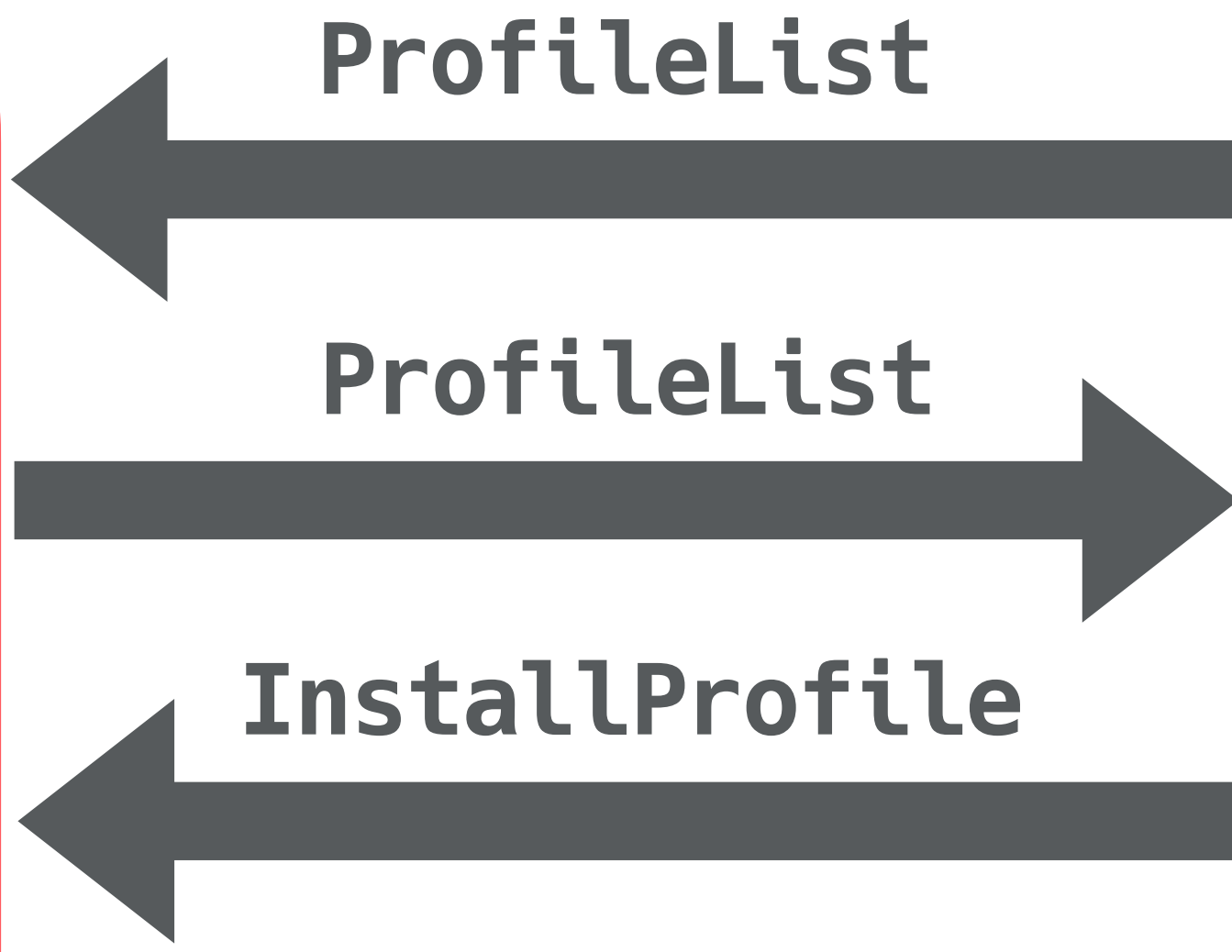
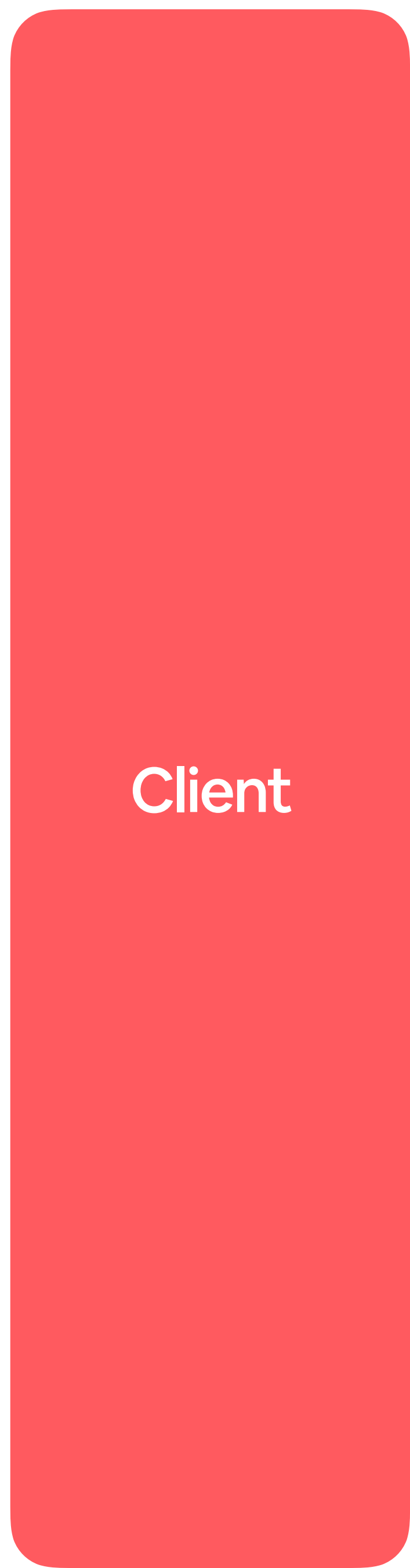
ProfileList

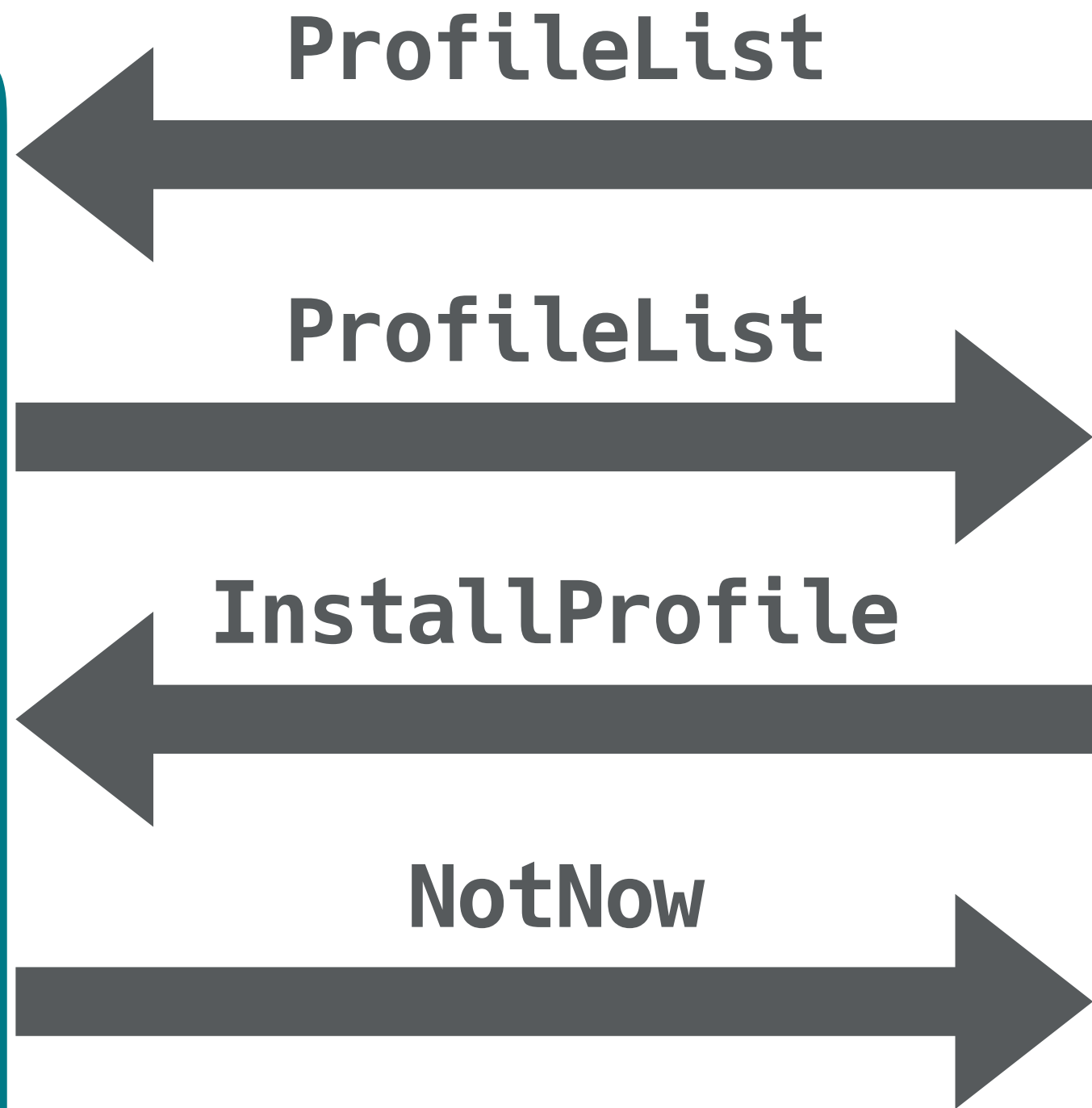
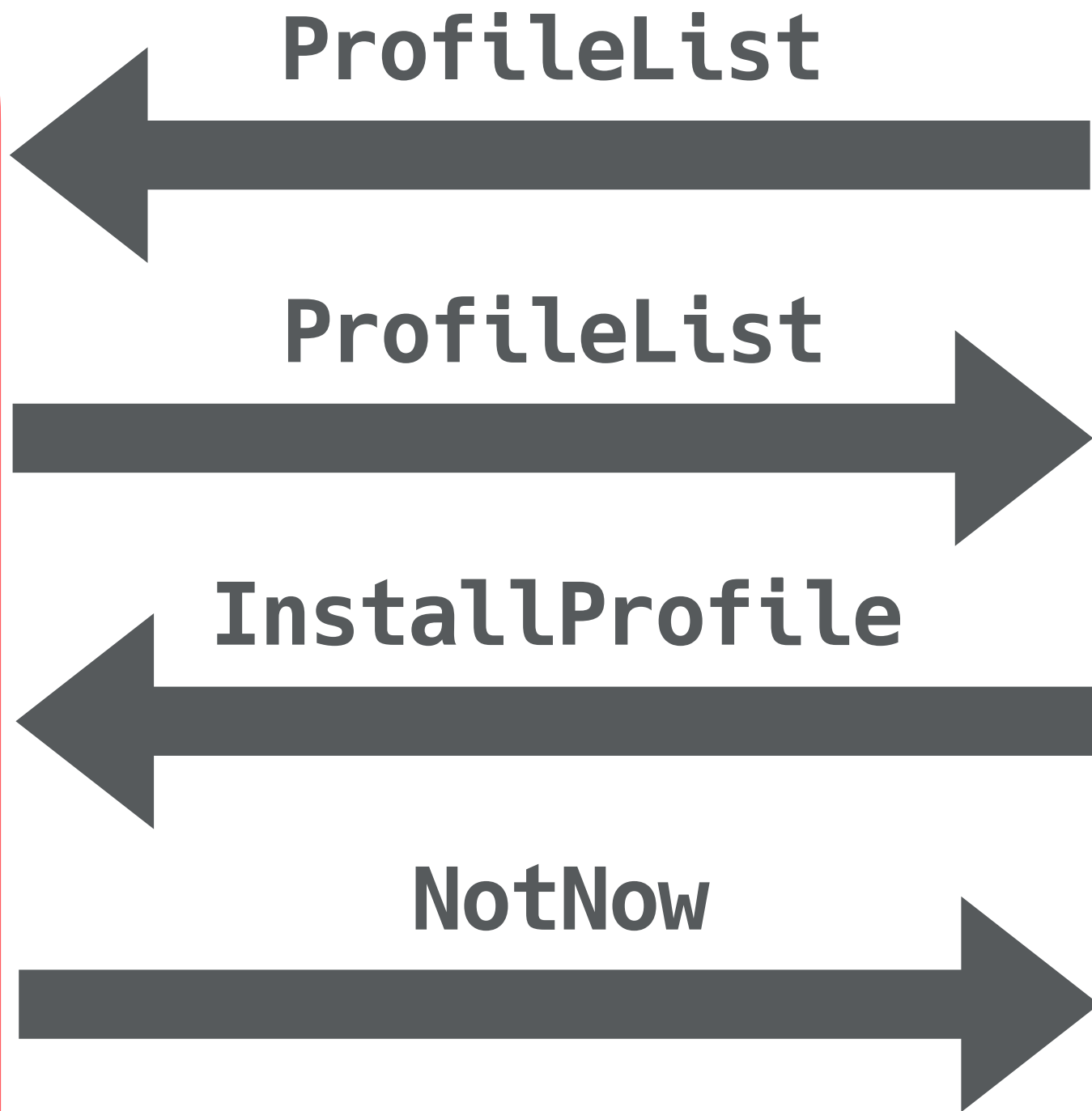
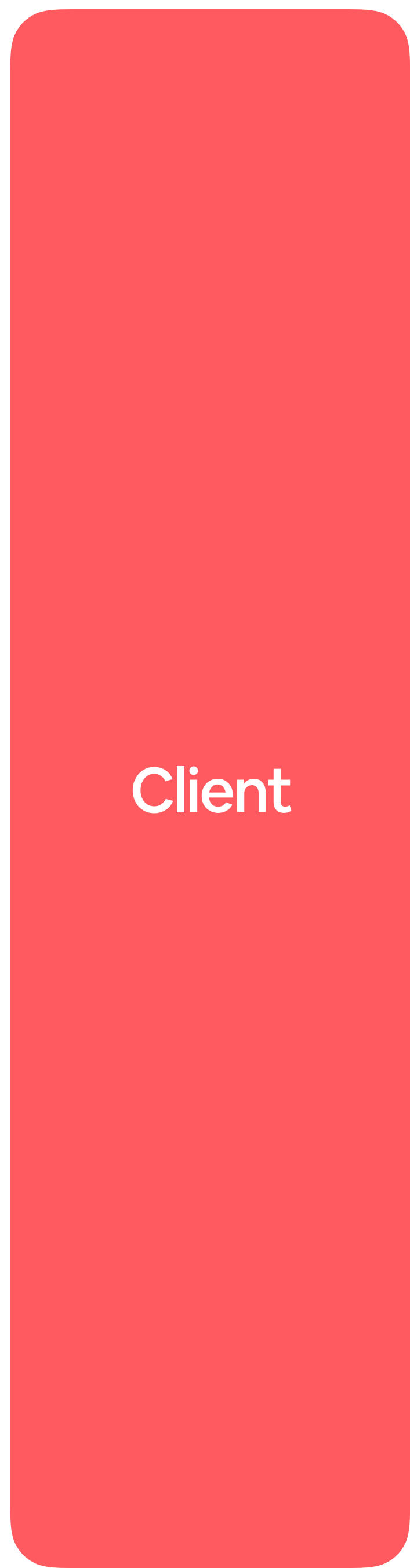


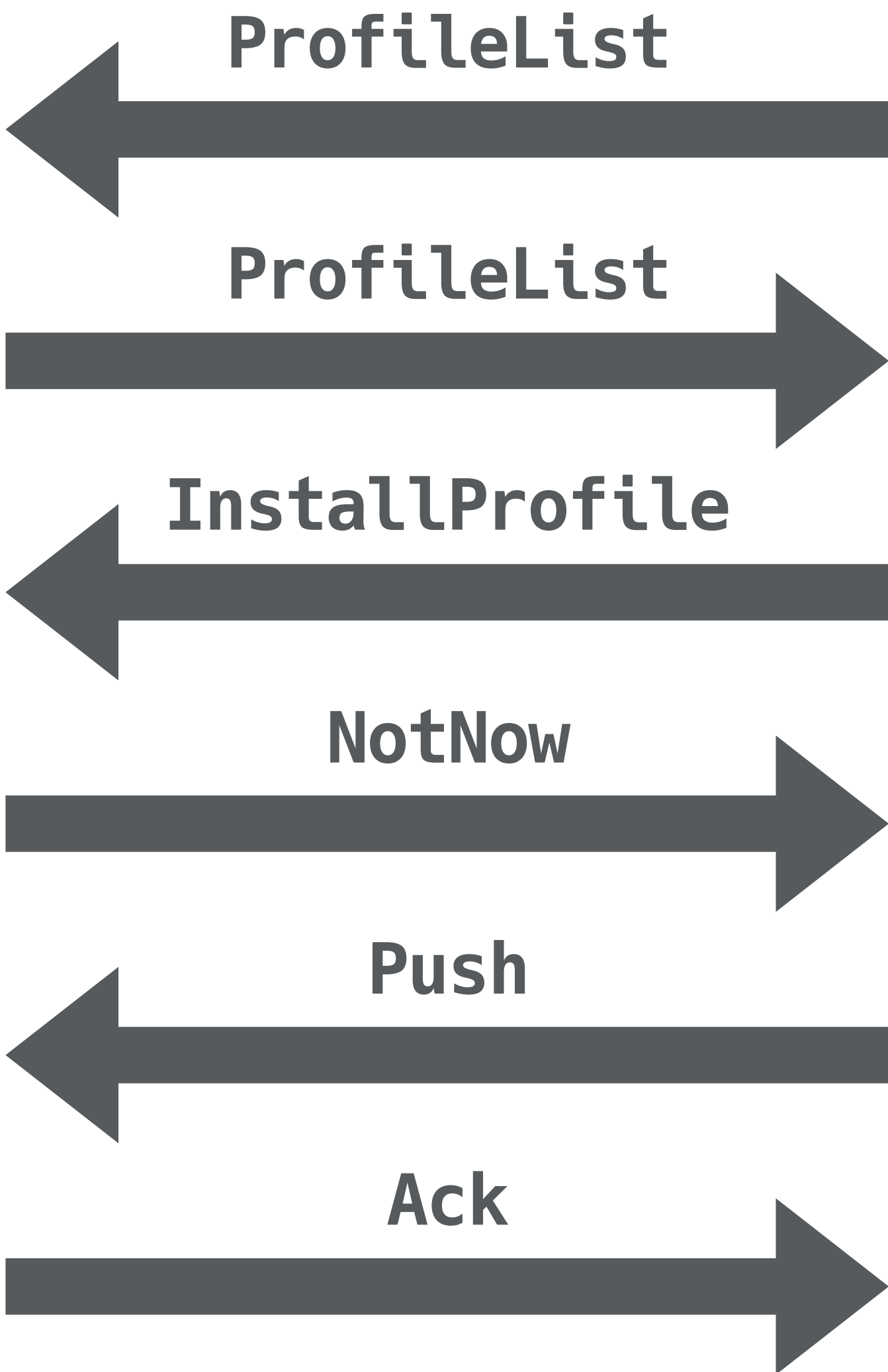
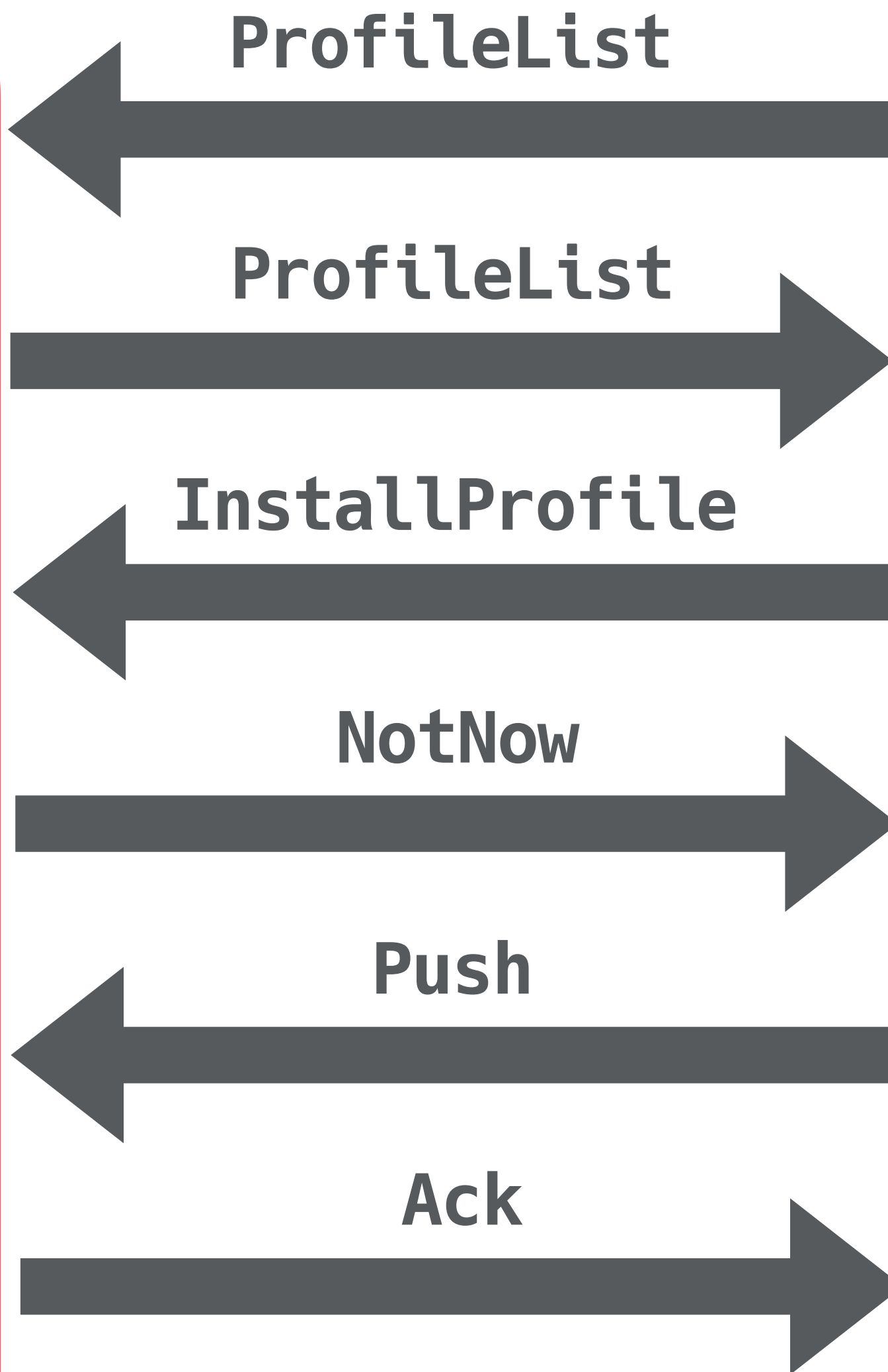
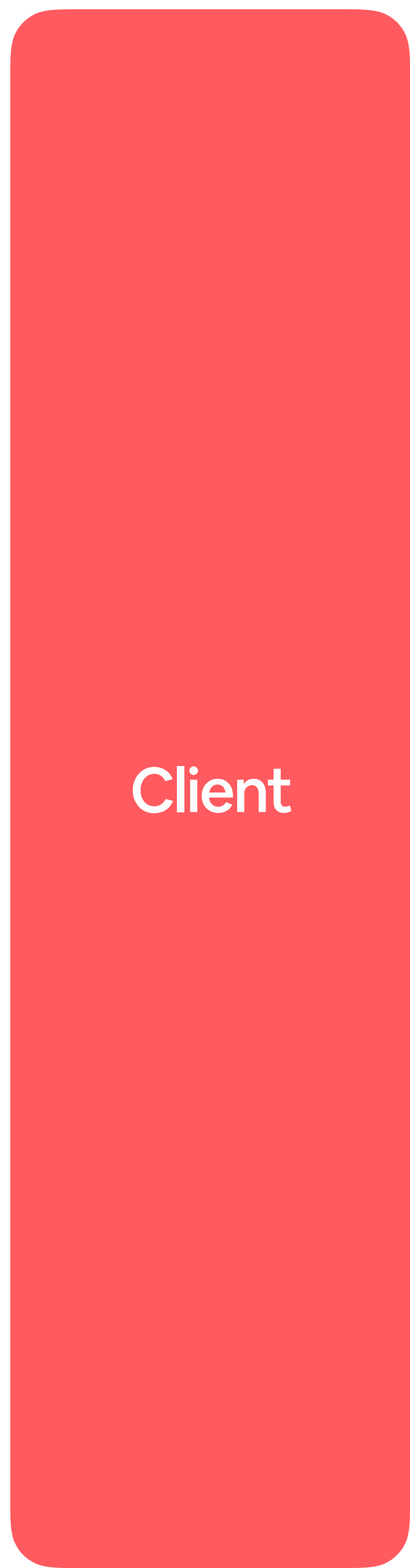
ProfileList

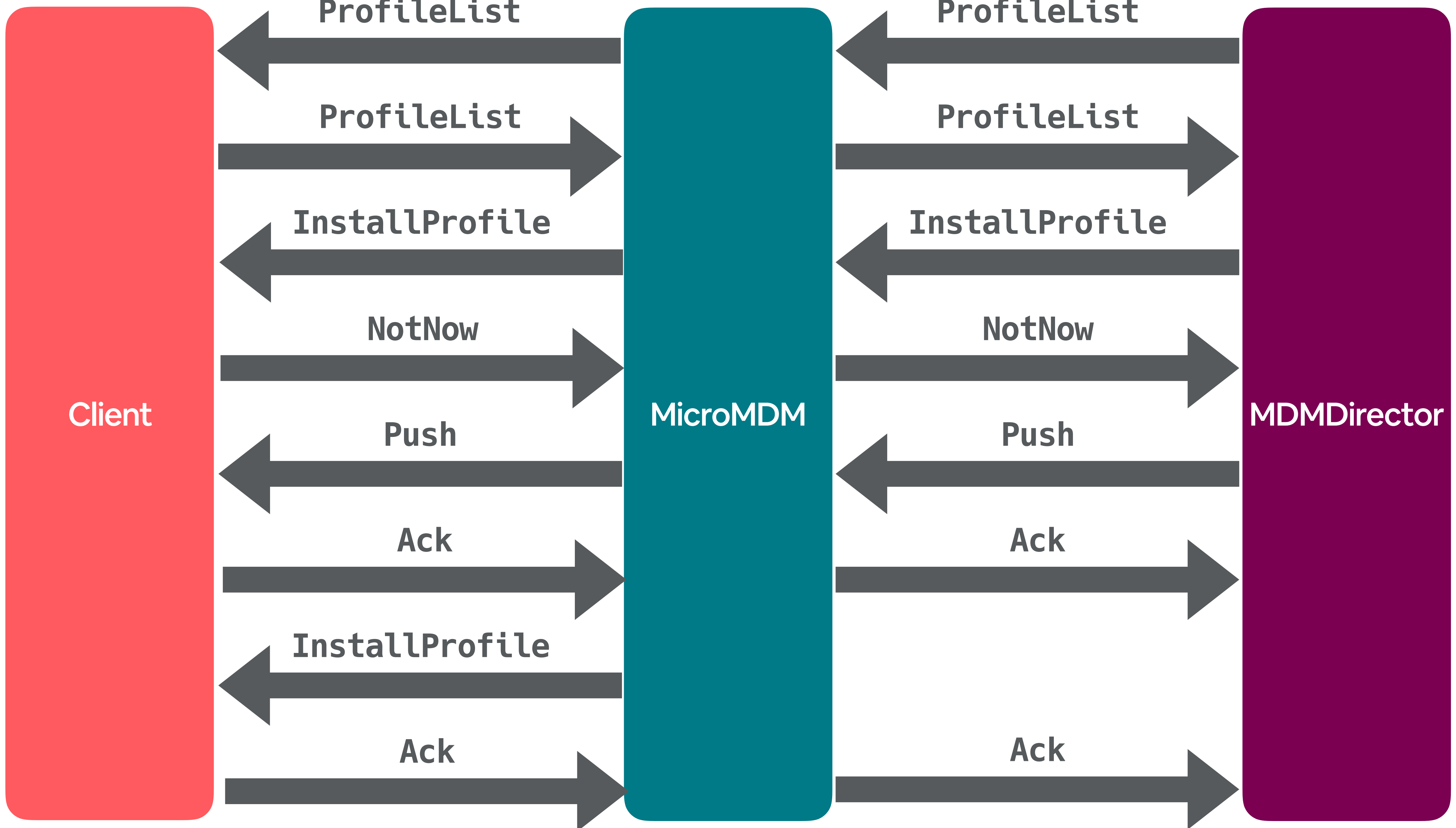












Client

MicroMDM

MDMDirector

ProfileList

ProfileList

ProfileList

ProfileList

InstallProfile

InstallProfile

NotNow

NotNow

Push

Push

Ack

Ack

InstallProfile

Ack

Ack

The future

- Control of more of the MDM spec (EraseDevice, DeviceLock)
- Tool to track state of applications to orchestrate InstallApplication
- Enrollment profile management (track installation and query cert expiry)

“Should I implement MicroMDM?”

Probably not.

Thank you!

- We are hiring! careers.airbnb.com
- MDM is woefully inadequate, but it's all we've got
- File feedback with Apple about what is missing
- graham.at/movember
- github.com/mdmdirector/mdmdirector
- #micromdm on MacAdmins Slack